NASA/TM—2010-216776 AIAA–2010–3469

A Risk Assessment Architecture for Enhanced Engine Operation

Jonathan S. Litt, Lauren M. Sharp, and Ten-Huei Guo
Glenn Research Center, Cleveland, Ohio

July 2010

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to *help@sti.nasa.gov*

- Fax your question to the NASA STI Help Desk at 443–757–5803

- Telephone the NASA STI Help Desk at 443–757–5802

- Write to:
  NASA Center for AeroSpace Information (CASI)
  7115 Standard Drive
  Hanover, MD 21076–1320

NASA/TM—2010-216776 AIAA–2010–3469

A Risk Assessment Architecture for Enhanced Engine Operation

Jonathan S. Litt, Lauren M. Sharp, and Ten-Huei Guo
Glenn Research Center, Cleveland, Ohio

Prepared for the
Infotech@Aerospace 2010 Conference
sponsored by the American Institute of Aeronautics and Astronautics
Atlanta, Georgia, April 20–22, 2010

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

July 2010

Acknowledgments

The authors gratefully acknowledge the support of the NASA Aviation Safety Program's Integrated Resilient Aircraft Control project.

Level of Review: This material has been technically reviewed by technical management.

Available from

NASA Center for Aerospace Information
7115 Standard Drive
Hanover, MD 21076–1320

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Available electronically at http://gltrs.grc.nasa.gov

A Risk Assessment Architecture for Enhanced Engine Operation

Jonathan S. Litt, Lauren M. Sharp, and Ten-Huei Guo
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

On very rare occasions, in-flight emergencies have occurred that required the pilot to utilize the aircraft's capabilities to the fullest extent possible, sometimes using actuators in ways for which they were not intended. For instance, when flight control has been lost due to damage to the hydraulic systems, pilots have had to use engine thrust to maneuver the plane to the ground and in for a landing. To assist the pilot in these situations, research is being performed to enhance the engine operation by making it more responsive or able to generate more thrust. Enabled by modification of the propulsion control, enhanced engine operation can increase the probability of a safe landing during an in-flight emergency. However, enhanced engine operation introduces risk as the nominal control limits, such as those on shaft speed, temperature, and acceleration, are exceeded. Therefore, an on-line tool for quantifying this risk must be developed to ensure that the use of an enhanced control mode does not actually increase the overall danger to the aircraft. This paper describes an architecture for the implementation of this tool. It describes the type of data and algorithms required and the information flow, and how the risk based on engine component lifing and operability for enhanced operation is determined.

I. Introduction

IN 1989, a McDonnell Douglas DC-10, United Airlines flight 232, suffered an uncontained failure in the tail engine. The fan disk failed and disintegrated which caused pieces of the structure to strike and destroy part of the tail and the horizontal stabilizer. As a result of this failure, all three of the hydraulic lines were cut, allowing the hydraulic fluid to drain away, disabling the flight control surfaces (i.e., ailerons, rudder, and all other flaps used to steer and control speed of the aircraft). Thus the pilots were forced to use the wing-mounted engines to steer the plane, using differential thrust to turn, and using additional or less thrust to control altitude. One of the serious problems the pilots faced was controlling the phugoid mode (long period pitch oscillations resulting in speed and altitude variations) which the control surfaces normally damp out. The pilots were able to learn to control this mode (to some extent) with properly timed changes in thrust (the delay time was as much as 20 to 40 seconds). Upon approach, the pilots found it was difficult to stay lined up with the runway. Additionally, the plane was coming in fast at 215 knots indicated air speed with a high sink rate of 1620 feet per minute. The plane crash landed and 111 of the 296 on board were killed in the accident; however it is remarkable that this many lives were spared considering the circumstances.[1]

In August 2006, a Bombardier Canadair Regional Jet CRJ-100ER, Comair Flight 5191, was assigned to take-off on Runway 22 of Blue Grass Airport, Lexington, KY. The pilots instead mistakenly used Runway 26, which was far too short for a safe takeoff, resulting in the aircraft overrunning the end of the runway before it could become airborne. The aircraft collided with terrain, trees and a fence, killing forty-nine people on board. Post-crash analysis indicated that the aircraft had not quite reached takeoff speed when impact occurred. It was also concluded that the flight crew realized something was wrong, but beyond the point at which the airplane could be stopped on the remaining available runway.[2]

Both of these catastrophes could have potentially been avoided if the engines had had the ability to respond faster or provide additional thrust. These and similar accidents demonstrate the desirability of enhanced propulsion control modes for in-flight emergency situations.[3] However, high-bypass gas turbine engines (these are the main engines used for large transport aircraft) are designed to provide safe and efficient operation over a long life. As a result, they accelerate slowly to minimize exposure of parts to extremely high temperatures and to minimize the chance of

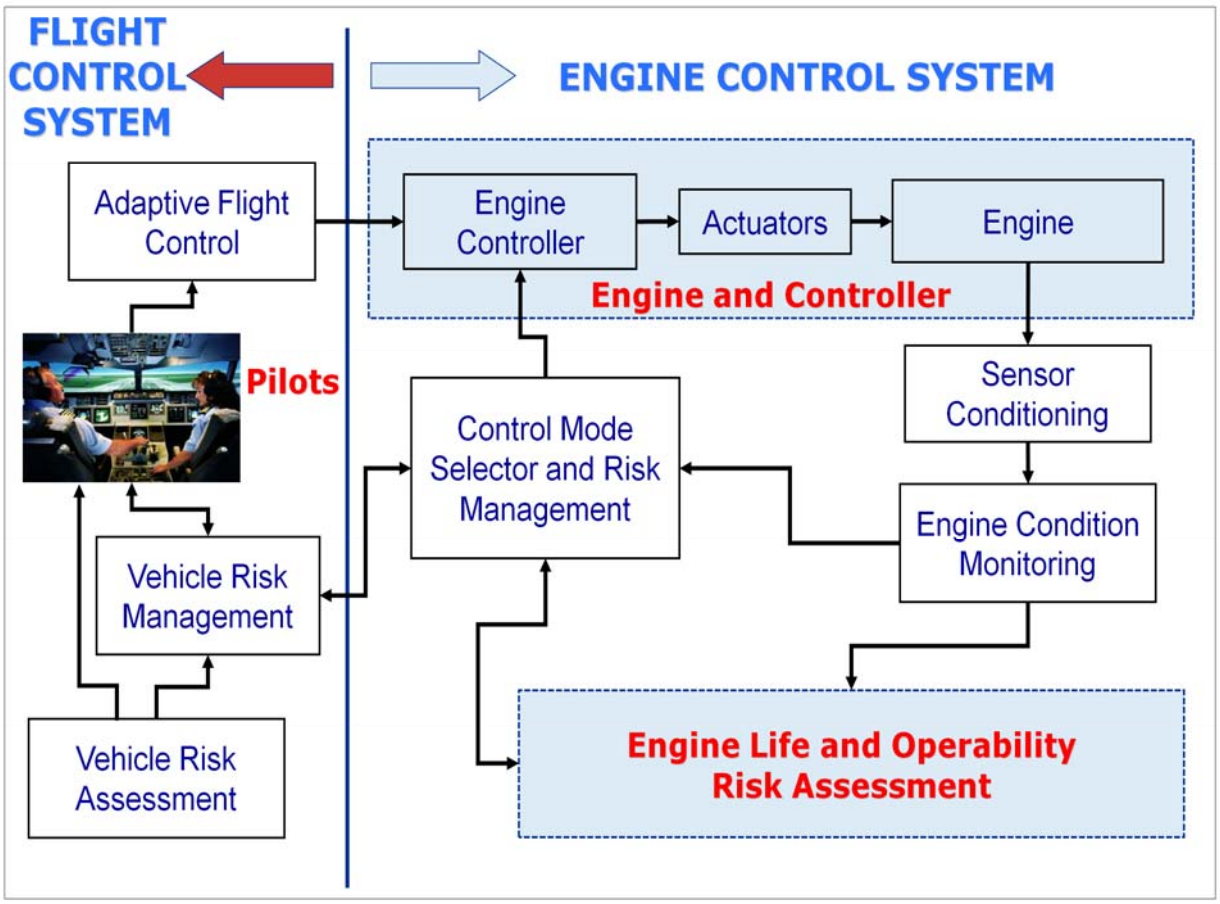

Figure 1. Risk Management Architecture.

stall. Since the deployment of an enhanced control mode for emergency operation could pose some danger to the engine, the risk of such an action under the given circumstances should be evaluated.

A Risk Management Architecture has been proposed for enhanced engine operation under emergency conditions.[4] The function of the Risk Management Architecture is to coordinate the engine control system with the flight control system to find the propulsion control mode or overall reconfiguration strategy that gives the airplane the best chance for a safe recovery in an emergency. This involves weighing the risk of an unsuccessful landing with the risk of implementing the enhanced control mode. The use of an enhanced control mode is intended to improve the chance of a safe landing, but will in general be more dangerous than using the standard propulsion control. This Risk Management Architecture, shown in Figure 1, contains multiple components or subsystems. The *Engine Life and Operability Risk Assessment* block contains the Risk Assessment Architecture, which is the subject of this paper. This subsystem evaluates the risk of performing a particular control action, specified at a higher level in the Risk Management Architecture. The *Engine Life and Operability Risk Assessment* block accepts requirements for the enhanced engine operation including the risk that the flight control system is willing to accept, and estimates the risk of using the specified control mode under the given circumstances. It returns information useful in decision making, such as the risk that will be incurred by performing the action, and limits on the control action so that the acceptable risk level will be met if the requested action's risk would exceed it.

The remainder of this paper is organized as follows. The FAA requirements for engine performance and operability are described, and these requirements are then related to the prognostic approach. Enhanced engine operation is discussed next. This is followed by a description of the components that make up the Risk Assessment Architecture, after which examples are presented demonstrating the information flow in two representative, hypothetical enhanced control modes.

II. Engine Life and Operability Prognosis

The Federal Aviation Administration (FAA) has mandated that engine components, both rotor and major static structural parts, be considered "life-limited" if their primary failure "is likely to result in a hazardous engine effect,"[5] and thus these parts must be removed from service at an approved life before hazardous engine effects can occur. A hazardous engine effect has the potential to be catastrophic; it is one that, among other things, results in non-containment of high-energy debris (e.g., disk burst), failure of the engine mount system leading to inadvertent engine separation, or uncontrolled fire.[6] The safe life of these life-limited parts must be determined by the manufacturer such that hazardous engine effects (which could be due to cascading failures) are predicted to occur at a rate not in excess of that defined as extremely remote (probability range of 10^{-7} to 10^{-9} per engine flight hour). The probability of a hazardous engine effect arising from an individual failure should be predicted to be not greater than 10^{-8} per engine flight hour. Thus, when seeking to certify an engine, the applicant must analyze it to assess the likely consequences of all failures that can reasonably be expected to occur. Normal engine operation will naturally promote certain failure modes such as high- and low-cycle fatigue, creep, etc., and the manufacturer's analysis must account for variations in the assorted factors that influence life, and the interaction between these factors. An engine failure in which the only consequence is partial or complete loss of thrust or power is considered a minor engine effect; although this is an undesirable event, it is not likely to be catastrophic under normal circumstances, and if it occurs in only one engine of a multi-engine aircraft it might be of little consequence. By definition then, an effect whose severity falls between hazardous and minor is regarded as a major engine effect, and the manufacturer's analysis must show that they are predicted to occur at a rate not in excess of that defined as remote (probability range of 10^{-5} to 10^{-7} per engine flight hour). These characterizations are useful because they classify the severity of failure modes and demonstrate that a quantifiable risk can be associated with these failures. Certification additionally requires some limited operational testing of rotating components beyond normal maximums to demonstrate integrity,[7] so while the failure risk in these cases cannot be sensibly estimated in numerical terms, the tests appear to establish a minimum safe life at these conditions.

The FAA also requires testing to certify that an engine can accelerate from low to high power within a specified time, and additionally that the engine can accelerate without experiencing overtemperature, surge, stall, or other detrimental factors.[8] This means that the controller must be designed to achieve a minimum performance in terms of transient response, while protecting the engine's operability by ensuring safe operation during extreme throttle excursions. Not only that, the controller is designed such that it will maintain these standards throughout the life of the engine, even though the engine is subject to normal wear and tear that makes it more susceptible to stall and overtemperature as it ages. This type of robust design essentially guarantees the engine's operation between overhauls under normal use. One can infer from this that a new engine might have the ability to respond faster without any detrimental effects, if the controller demanded it, since a deteriorated engine is still capable of operating safely. Nonetheless, it is common practice to limit the acceleration of turbofan engines to a standard profile in multi-engine aircraft, one that even the most deteriorated engine can achieve, in order to reduce the impact of mismatched engines and thereby minimize the potential for yaw on take-off.[9]

The FAA's certification requirements for engines take into account life, performance, and operability. These three attributes are evaluated independently, but are intimately tied together in practice. The safe life of life-limited parts is determined based on normal use, which is related to the steady state and transient performance of the engine, realizing that as the engine wears it runs hotter. The exhaust gas temperature is a gauge of engine deterioration, and it is used to indicate when maintenance is required; this presumably limits the maximum temperatures the internal engine components will experience. The operability of the engine is also related to how the engine deteriorates with use. Engine performance is maintained during large transients even as the engine ages, albeit with less available stall margin. Thus the closed-loop system must be designed with enough stall margin to deliver consistently acceptable response, which means that the maximum amount of stall margin debit due to deterioration between overhauls can be anticipated. Thus, under normal operation, the engine is well-characterized in terms of life, performance and operability.

Under normal circumstances, the conservative design of the engine's controller enables the engine to have long on-wing life and robust operation. In the case of an emergency, such as loss of flight control capability or runway incursion, allowing the engine to take advantage of its reserve capabilities could provide the extra boost required to save the plane from crashing. However, once the controller is modified to allow the additional responsiveness, there is no longer any guarantee of safe operation. Faster response leads to potential stall, and greater-than-normal thrust can lead to dramatically shortened life. Even a minor engine effect (recall that this is defined as partial or complete loss of thrust) could become catastrophic when the engine is being relied upon to maneuver the aircraft out of harm's way. Therefore, the ability to modify the controller to take advantage of the unused performance and operability margin must be coupled with a way to determine the risk of performing the requested action, and that risk can then be weighed against the risk to the vehicle if the action is not performed.

III. Enhanced Engine Operation

The propulsion system's enhanced control modes are based on the types of emergencies that have occurred historically for which greater capabilities could have potentially improved the probability of safe recovery. Based on the previously described scenarios, beyond-normal thrust (overthust) and faster-than-normal control responses are being considered. There may be multiple ways to achieve these types of responses, so any individual control mode is a specific approach to meet the requirement. Naturally the way the objective is met will determine the likely failure modes, so specific failure modes must be determined for each control mode. For instance, attempting to achieve a faster-than–normal thrust response by modifying the engine controller's limit logic might result in high pressure compressor (HPC) stall on acceleration (operability). Higher-than-normal thrust produced by allowing excessive rotational speed could result in failures such as disk burst and stress rupture failure of the blades (life).

When an emergency situation is recognized, the flight controller portion of the Risk Management Architecture (Figure 1) evaluates the situation and determines the engine requirements for enhanced operation that will improve the chance for recovery or safe landing. The enhanced engine capability might, for instance, make the vehicle reasonably maneuverable despite damaged flight control surfaces. From the point of view of the flight control, the engines are merely actuators, and if they can provide the requested response the situation is less dire. However, enhanced engine operation is inherently risky. There might be various enhanced control modes available to achieve a desired response, or various degrees of achieving it; this is up to the *Control Mode Selector and Risk Management* block to determine. To facilitate this, the flight controller must specify the level of risk it is willing to accept with enhanced engine operation so that the overall chance of survival is maximized. Thus the flight controller's performance request is converted into a proposed enhanced control mode with specifications about its implementation. If it is determined to be too risky, other control modes can be evaluated, initiated by the *Control Mode Selector and Risk Management* block, or the flight controller's performance requirements or acceptable risk can be modified. This iteration and negotiation to arrive at an appropriate response with an acceptable risk is the function of the Risk Management Architecture. The risk determination for any specific enhanced control mode is performed by the Risk Assessment Architecture.

IV. Risk Assessment Architecture

The purpose of the Risk Assessment Architecture is to evaluate the risk of performing a specified action under the given circumstances. This is accomplished through the use of sets of algorithms specific to the enhanced control modes. These algorithms, which are designed to address each of the developed enhanced control modes based on the given engine and airframe combination, fit within the generic Risk Assessment Architecture. Although there are two distinct concerns—life and operability—the primary output of the *Engine Life and Operability Risk Assessment* block is a risk level, so whether it is a risk to life or operability or a combination of both, the result is a likelihood or probability. Thus the architecture provides a generic structure in which to compute risk, independent of cause or effect.

The Risk Assessment Architecture has three main components: the database of engine characteristics required for risk calculation; a set of algorithms to determine risk based on the various enhanced control modes; and the on-line, real-time information computed based on (normal) past use and anticipated enhanced use in an emergency situation. The set of algorithms to determine risk operates on the database of engine characteristics so that together they produce the on-line, real-time information. The Risk Assessment Architecture is shown in context in Figure 2. The three components comprising it are described next.

A. Database of engine characteristics

The database of engine characteristics contains information specific to the engine, such as number of disks, diameter of each disk, number of blades per disk, material properties, etc. This is general information about the engine, independent of any specific enhanced control modes, that can be used for computing risk of operation for any given control mode. The type of information required to be contained within the database will, of course, depend upon the control modes that need to be analyzed, but the information itself is fundamental. The cross section of a turbofan engine is shown in Figure 3. In the figure, the air moves from left to right, through the fan which generates most of the thrust by pushing a large amount of air through the bypass duct (the large diameter annulus on the left). A small percentage of the air travels through the core (the part behind the fan that extends to the right) and is compressed, mixed with fuel and burned, and then expanded out through the turbine, driving the fan. Under

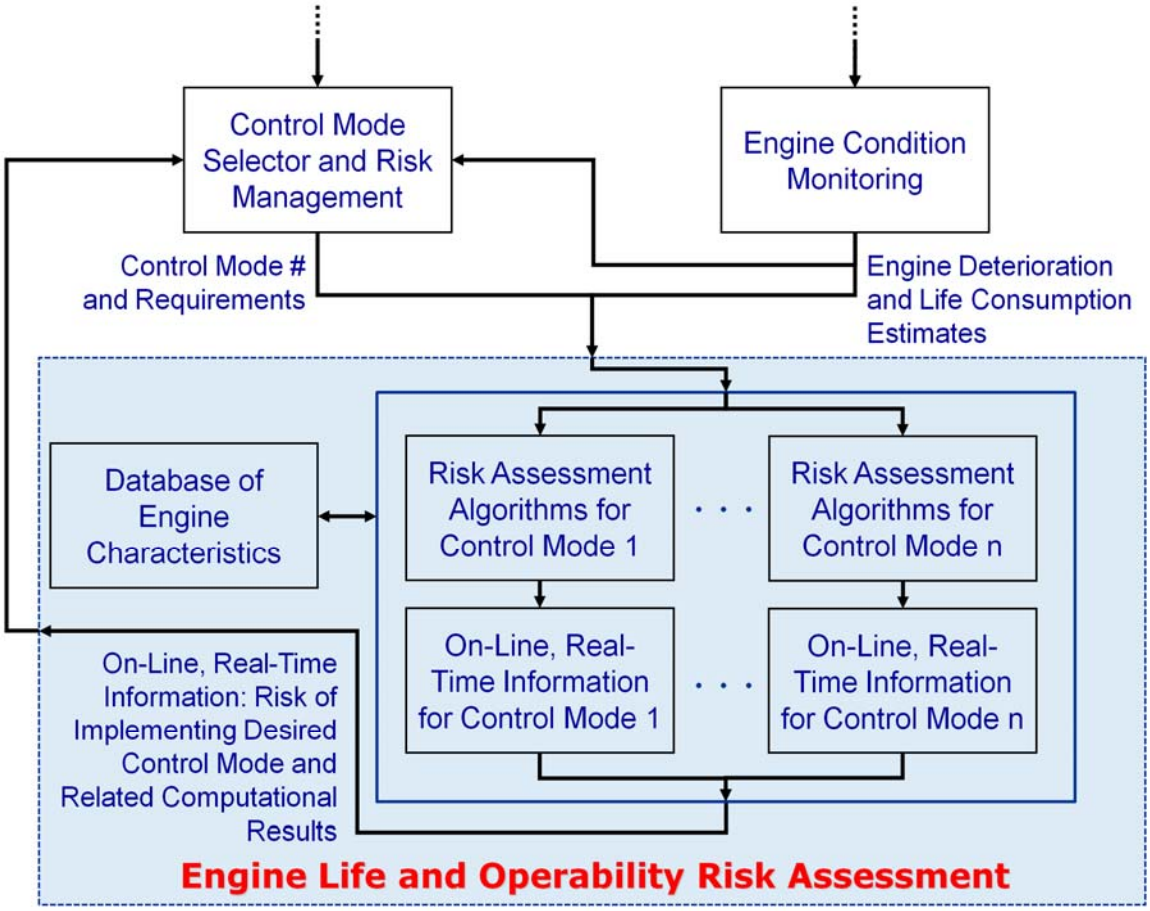

Figure 2. Block Diagram of the Risk Assessment Architecture (the framework of the *Engine Life and Operability Risk Assessment* block) as a subset of the Risk Management Architecture (Figure 1).

normal conditions, the moving parts of the engine, which can weigh several thousand pounds in total, rotate about the central horizontal shafts at speeds of thousands of rpm, and the temperature of the hot gas can be well in excess of 2000° F. Clearly the potential for catastrophic damage exists if the engine is driven beyond its safety limits.

The FAA currently requires that lifing analysis be performed on parts whose failure can result in a hazardous engine effect under normal use. Failure modes that can reasonably be expected to occur and would result in hazardous engine effect under enhanced use can be analyzed in the same way. For example, Figure 4 shows the life distribution of turbine blades of a given material for a range of temperatures and stresses.[10] The life decreases exponentially as temperature and stress (which is a function of rotational speed) increase. Figure 5 shows the relationship between the life of a particular kind of disk and rotational speed.[11] Here again life decreases exponentially with speed. These two figures are examples of the type of information that might be required to calculate the risk of operating in an overspeed control mode to produce additional thrust.

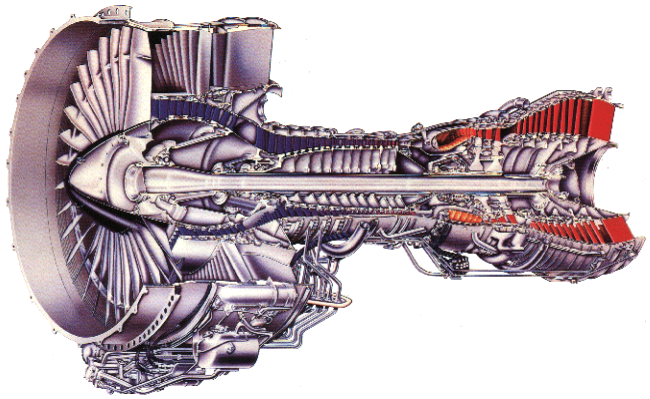

Figure 3. Turbofan engine cross section.

B. Risk assessment algorithms for enhanced control modes

The algorithms that determine risk due to exercising a specific control mode are naturally control mode dependent. Since the possible enhanced control modes are known, the

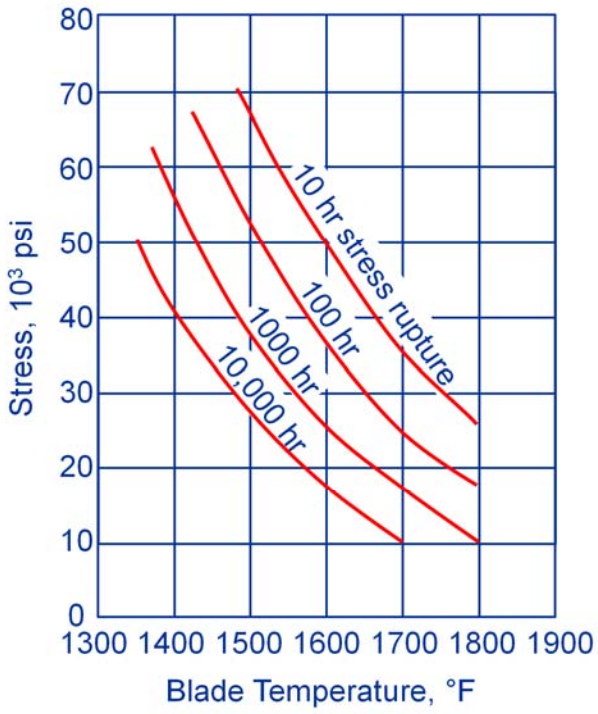

Figure 4. Example turbine blade material life based on stress and temperature.

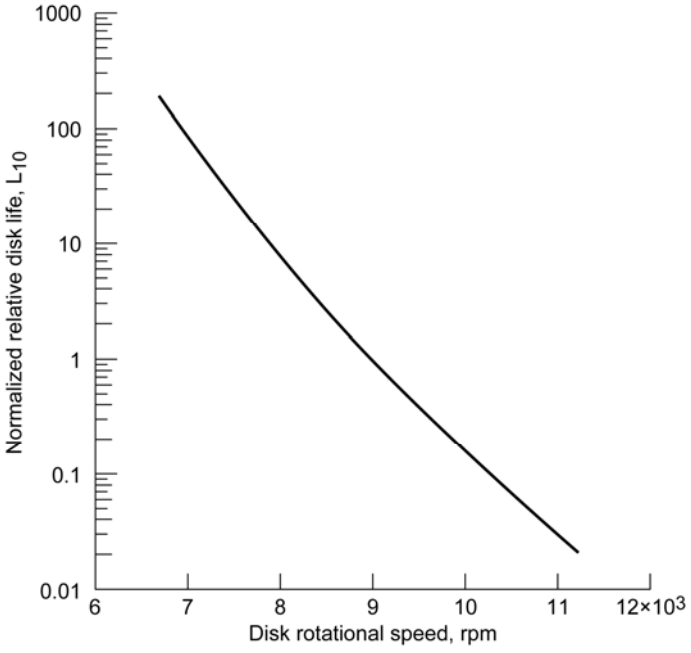

Figure 5. Example normalized characteristic life of a disk as a function of rotational disk speed.

algorithms required for computing the risk associated with their deployment are preprogrammed. Thus the request to initiate a specific enhanced control mode automatically starts the process of activating the correct algorithms. Different failure modes might be dominant if the engine is stressed in different ways, and the risk of failure is related to the failure mode excited and how it manifests itself. The algorithms can include physics-based models of structural life, or statistical tests, and they use the information contained in the database as well as current information about the engine's state and future operation.

C. On-line, real-time information

The on-line information generated by the *Engine Life and Operability Risk Assessment* block is a risk of performing a certain operation, information related to the risk or to the acceptable risk, or some information used to help compute the risk. The information is produced by applying the algorithms to the contents of the database, with the situation-specific details that make the results relevant.

V. Information Flow

The Risk Assessment Architecture has been described in general terms, but the information flow is most easily demonstrated through the use of examples. At a high level, the risk factors of concern are stall and component failure, the first would usually be expected to occur during fast response, and the second during overthrust. Of course the risk depends on the implementation of the enhanced control mode, but for demonstration purposes we will assume that a specific control mode exists for each type of operation. A flow chart for the risk assessment process is shown in Figure 6. In the following descriptions, hypothetical control modes are described; these example computations are the type that would be carried out in a real implementation.

A. Fast response control mode

For a large rapid throttle movement, the controller limit logic will usually determine the engine's thrust response time.[12] The limit logic usually contains some type of acceleration schedule. A common type of acceleration schedule, known as NDOT,[13] specifies core acceleration as a function of core speed. This is because at low speed, the high pressure compressor (HPC) is likely to stall during rapid

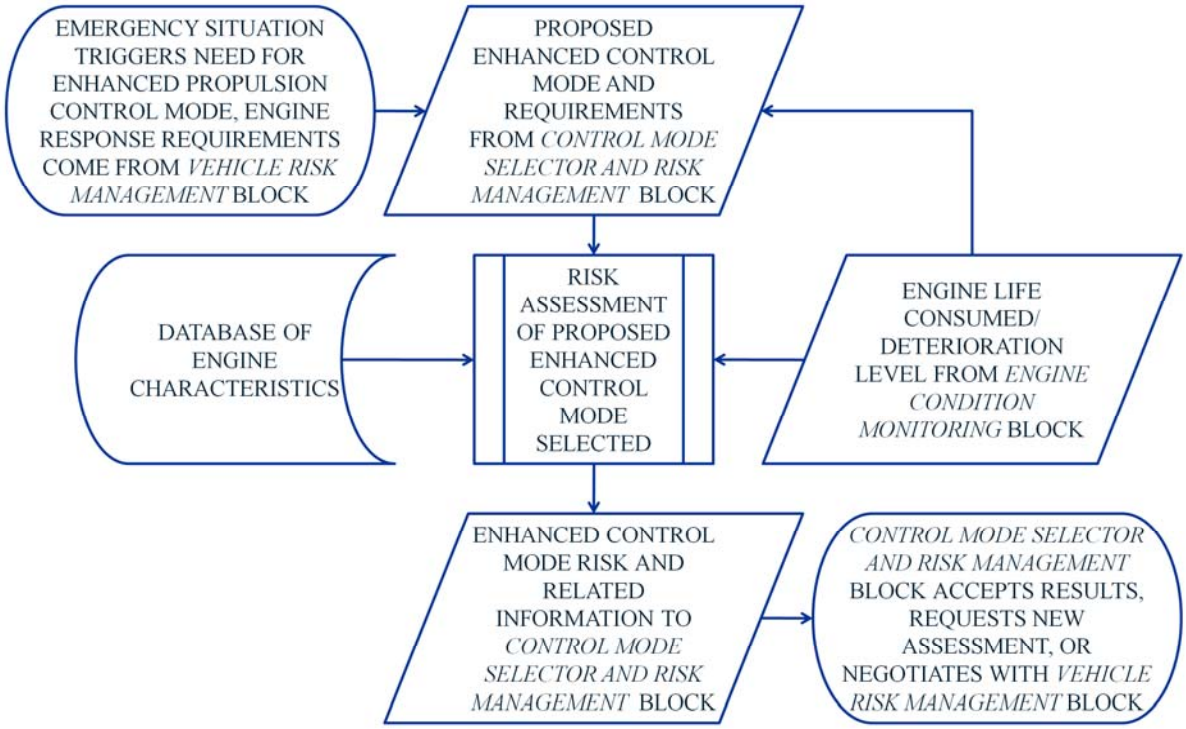

Figure 6. Flow chart of the risk assessment process for the use of enhanced propulsion control. The risk assessment algorithms are predefined based on the control mode selected.

accelerations and so it must be tightly controlled. The HPC is designed such that its operating line is far enough from its stall line to ensure that it will never stall under normal operation; this distance, called the stall margin (SM), is defined in Figure 7. The required stall margin consists of a stack-up of several components, the largest of which is the transient allowance, i.e., the amount set aside for the temporary stall margin decrease due to transient operation. The size of the dip in stall margin due to the transient depends upon the speed of response—the faster the response, the larger the dip (Figure 8).[14] As previously stated, the propensity to stall is related to the level of engine deterioration, and a new engine often has the capability to accelerate more quickly than an older engine. However, the acceleration schedule must be designed for any engine of the same type in the fleet, and be valid throughout the engine's life, therefore it must allow even the most deteriorated engine operating under the worst conditions to accelerate safely. The Risk Management Architecture (Figure 1) contains a block called *Engine Condition Monitoring* that feeds into both the *Engine Life and Operability Risk Assessment* and the *Control Mode Selector and Risk Management* blocks. For this example, the *Engine Condition Monitoring* block would contain algorithms that might estimate the level of deterioration of the engine, or even a measure of how close the engine's operating line is to stall.[15,16] Now, say that a family of acceleration schedules has been developed, appropriate for various levels of engine deterioration, and the most conservative schedule is the nominal schedule used in the controller. If the damaged flight control system determines that to damp the phugoid mode, for instance, the engine response time constant must be decreased to some particular value, the *Control Mode Selector* might request an evaluation of the risk of using a more aggressive acceleration schedule that would produce such a response, at the cost of a smaller stall margin transiently. The *Engine Life and Operability Risk Assessment* block would use the estimate of engine deterioration generated by the *Engine Condition Monitoring* block, as well as information about the accuracy of that estimate, to determine if the risk of implementing that acceleration schedule is acceptable according to what the flight control system has specified.

Reference 9 lists the contributors to the HPC stall margin worst case stack-up, i.e., the various factors that must be accounted for to ensure that the engine does not stall on acceleration; they are shown in Table 1. The total of 24.4% indicates the distance the HPC's designed steady state working line must be from the stall line in order to ensure safe operation throughout the life of the engine under normal use. Some of the components of the stack-up are random, the remaining are systematic deviances related to deterioration or type of operation. Potentially some of

Table 1. Example of stall margin stack-up for the HPC

Cause	Systematic Deviances	Random Variances
New production engine-to-engine working line variation	0	± 1.5%
New production engine-to-engine stall line variation	0	± 4.0%
In service working line deterioration	-2.0%	
In service stall line deterioration	-4.0%	
Control system fuel metering, and other actuators	0	± 1.0%
Reynolds number effects	-1.0%	
Inlet distortion	-1.0%	
Transient allowance	-12%	
Total	-20%	± 4.4%

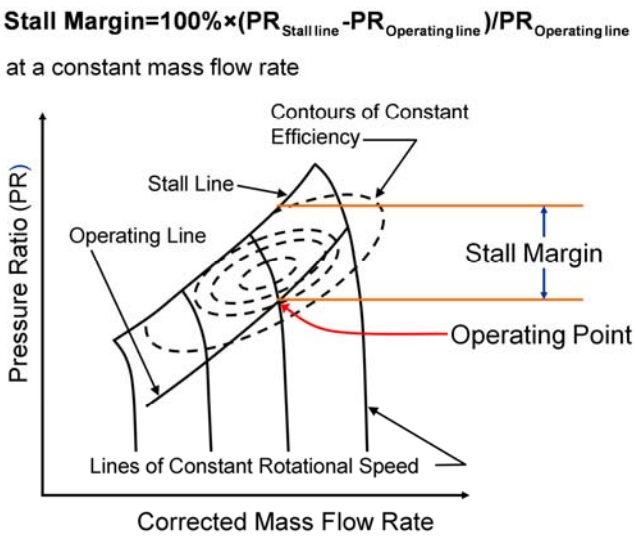

Figure 7. Pressure Ratio (PR) of HPC vs. Mass Flow Rate, showing how Stall Margin (SM) is defined.

the latter group can be estimated. The deterioration-related stall margin debits would be estimated and made available by the *Engine Condition Monitoring* block, and the inlet distortion might be able to be estimated using airframe parameters such as angle of attack and sideslip. This type of information enables the required stall margin reserve to be reduced because the portion required for each component of the stack-up that is estimated will usually be less than its corresponding worst case (three sigma) stall margin set-aside. This means that it is known with some confidence that the whole reserve is not required and the unneeded portion may now be utilized for the transient.

Let us assume that each of the components of the baseline stall margin stack-up shown in Table 1 represents a worst case (three sigma), and that each is independent (after lumping the two deterioration debits together), and that there exists an unbiased estimator for those non-random components of the stack-up that are able to be determined. Furthermore, let us assume that the random components of the stack-up and the estimation errors are independent and normally distributed random variables. The portion of the stack-up due to random components (engine-to-engine working line and stall line variation, and actuator variation) is accounted for in the stall margin by utilizing the facts that 1) the sum of normally distributed variables is normally distributed, and 2) the variance of this sum of normally distributed random variables is the sum of the variances of the individual normally distributed random variables. Since the standard deviation is the square root of the variance, the standard deviation of the new distribution is easily determined from those of the original distributions. Under normal circumstances, the one-sided three-sigma value might be used as the stall margin component due to random effects, as in Eq. (1).

$$\left(\left(3\sigma_1\right)^2+\left(3\sigma_2\right)^2+\left(3\sigma_3\right)^2\right)^{1/2}=\left(9\left(\sigma_1^2+\sigma_2^2+\sigma_3^2\right)\right)^{1/2}=3\left(\sigma_1^2+\sigma_2^2+\sigma_3^2\right)^{1/2}=3\sigma \tag{1}$$

With estimators for the other components of the stall margin stack-up, the risk can be bounded in a similar way, using the fact that the estimation error is a random variable. For instance, Ref. 16 describes an approach that has been demonstrated in simulation to produce an unbiased estimate of HPC stall margin with a standard deviation significantly less than the deterioration-induced debit. Incorporating any such estimation errors into the stack-up due to random variations (as in Eq. (1)), and setting the acceptable risk to, say, 3% (2σ) gives the equation

$$\left((2\sigma_1)^2 + (2\sigma_2)^2 + (2\sigma_3)^2 + (2\sigma_{estimation\ error})^2 \right)^{1/2} = 2\sigma \quad (2)$$

where 2σ corresponds to about 97% of the one-sided normal distribution, ensuring that the estimate of the deterioration-induced stall margin debit is greater than the actual debit with a probability of about 0.97 (see Figure 9). Note that the coefficients in Eq. (2) do not need to all be the same—for instance if nothing is known about a particular component of the stack-up it might be unwise to reduce its debit—as long as the acceptable risk from the resulting distribution is as specified.

The original required stall margin (worst case stack-up) is now known to be larger than necessary. The unnecessary amount is determined as the difference between the set-aside (worst case) and requirement for each estimated component, less the estimation uncertainty from Eq. (2). This part of the stack-up is now freed up to be used for the transient response. So, if the acceleration schedule required to produce the requested engine response generates a transient-related dip in stall margin that is less than the original transient allowance plus the unneeded portion of the original set-aside, the risk of implementing this acceleration schedule is less than the maximum acceptable risk.

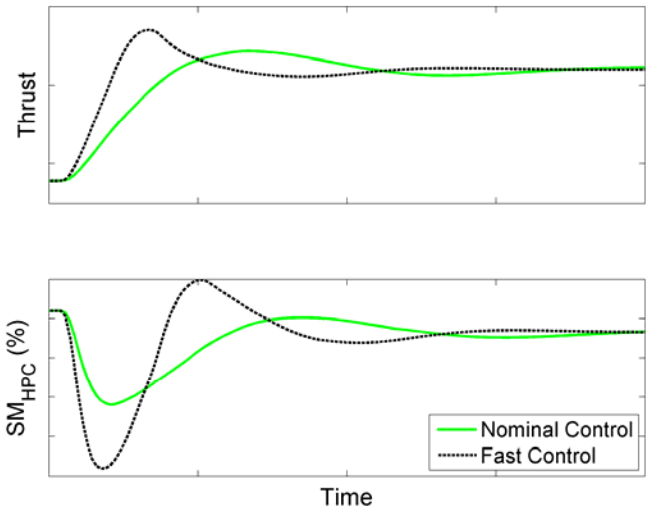

Figure 8. Nominal and rapid thrust response and corresponding HPC stall margin (SM) trajectories vs. time.

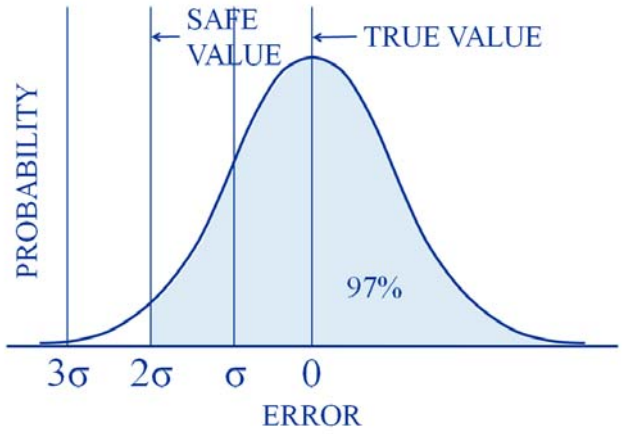

Figure 9. Normally distributed unbiased estimation error with 3% risk acceptable. This approach applies to any random component of the stall margin stack-up.

To synopsize this example demonstrating the information flow from Figure 6, say an aircraft's rudder locks, causing yaw control to be lost. The *Vehicle Risk Management* block from Figure 1 would request the *Control Mode Selector and Risk Management* block to implement a fast thrust response control mode to achieve yaw control with a specified bandwidth or time constant using rapid differential thrust modulation, without exceeding a given risk level. The *Control Mode Selector and Risk Management* block selects one of the pre-existing fast thrust response strategies to achieve it (modified acceleration schedule, in this example) and sends the specific schedule and acceptable risk to the *Engine Life and Operability Risk Assessment* block for analysis. The *Engine Condition Monitoring* block would provide an estimate of the engine's deterioration level that can be related to stall margin debit, as well as the uncertainty associated with the estimate. The algorithms in the Risk Assessment Architecture would combine the uncertainty information using Eq. (2) to generate an estimate of the risk of using the new acceleration schedule, and this would be returned.

B. Overthrust control mode

To implement an overthrust control mode we can assume an overspeed operational mode. Thrust is proportional to airflow through the engine, which is directly related to both Engine Pressure Ratio (EPR, defined as Low Pressure Turbine discharge pressure divided by inlet pressure) and fan speed, so it is common to use one or the other as the control variable.[13] Higher-than-normal thrust might be demanded due to, for instance, a shortened takeoff distance because of a runway incursion,[3] or significant in-flight wing damage that reduces lift on that side of the aircraft.[17] One way to achieve overthust is to increase the setpoint (fan speed or EPR) beyond the normal upper limit. If the higher-

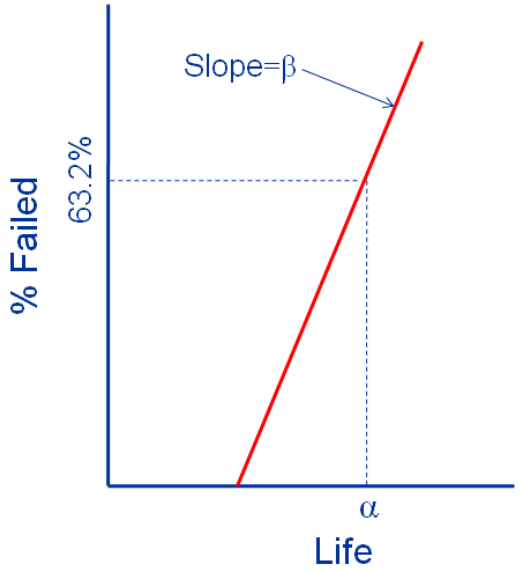

Figure 10. Two-parameter Weibull plot.

than-normal thrust level is required for more than a very short time, it is a steady state condition and component life becomes a concern. Even under normal circumstances, time at temperature is a limiting factor in engine operation. For instance, *maximum continuous thrust* is the maximum thrust at which the engine may operate continuously while the higher *takeoff thrust* is the maximum thrust at which an engine is allowed to operate for a five minute duration (based on maximum exhaust temperature).[13] This is because the stress on the hot section components at this condition tends to shorten their life significantly. Figure 4 and Figure 5 show examples of how the life is debited due to excessively harsh operation.

We assume that component life is probabilistic, meaning that for a population of parts that are exposed to the same conditions, there is a distribution of failure times. As discussed earlier, the safe life of a part is the time before which no failure can be reasonably expected to occur, i.e., the probability of a failure is extremely remote. When dealing with a population of turbine disks, for example, the removal time is dictated by the risk of the first failure, even though 80% of parts replaced at low-cycle fatigue (LCF) calculated safe-life limits have at least a full order of magnitude of fatigue life remaining.[18] This leads into the definition of risk. If the probability of the first failure occurring at the safe life is an acceptably low known value, and running for an additional 10 times as long as the safe-life limit results in only 20% of the disks having failed, then a two-parameter probability distribution, such as Weibull, can be generated as

$$F(t) = 1 - \exp\left[-\left(\frac{t}{\alpha}\right)^{\beta}\right], t > 0 \tag{3}$$

where α and β specify the distribution as shown in Figure 10. A Weibull plot is a Cumulative Distribution Function (CDF) that represents the probability of failure versus time using scaled axes so that the resulting line is straight. Weibull distributions are often used to represent failure behavior because they possess some important properties, and they have the versatility to suggest other distributions while retaining these properties. One important property is that Weibull distributions of individual components can be combined into a single Weibull distribution for an entire system as long as the β parameter for the individual distributions is equal. This is useful for simplifying the CDF for a large group of similar components such as disks or blades. Even when the β parameters are dissimilar and the CDFs cannot be combined, an analytical expression can be created for the CDF of system failures using the concept of survivability.

The survivability of a component, $S(t)$, can be defined as one minus the risk, $F(t)$, which is equivalent to one minus the CDF, as shown below,

$$S(t) = 1 - F(t) \tag{4}$$

One way to combine multiple independent failure distributions into a single distribution for the engine is by calculating the survivability in Eq. (5). Note that the independence assumption is justified since any individual failure of the level of severity considered here would be enough to curtail the use of the enhanced control mode in an emergency situation.

$$S(t) = (1 - F_1(t))(1 - F_2(t)) \cdots (1 - F_N(t)) \tag{5}$$

Since, by manipulation of Eq. (4), the risk $F(t)$ equals one minus the survivability $S(t)$, Eq. (6) represents system risk as a function of component life.

$$F(t) = 1 - (1 - F_1(t))(1 - F_2(t)) \cdots (1 - F_N(t)) \tag{6}$$

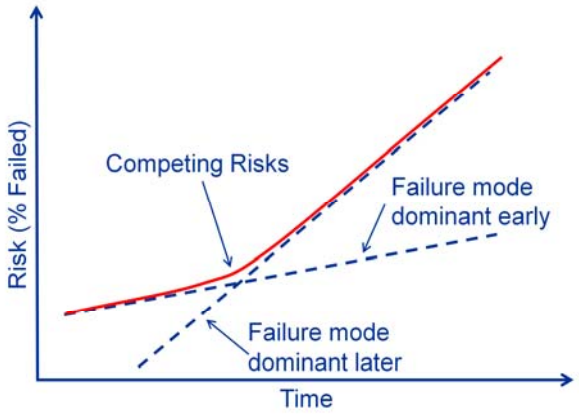

Figure 11. Weibull plot of risk of operation engine in normal then enhanced mode.

Note that, for analysis purposes, the individual risk terms of Eq. (6) corresponding to failure modes associated with enhanced operation might become nonzero only after the new control mode is initiated. Equations (4)-(6) are valid for any distribution, but the Weibull assumption simplifies the analysis.

Equation (6) describes the risk to engine life in terms of structural failures that would be catastrophic in an overthrust control mode. When there are competing failure modes or specific failure modes associated with enhanced operation, the Weibull plot of the CDF may look more like that in Figure 11, but the analysis is the same.

As an example to demonstrate the information flow shown in Figure 6 for an overthrust control mode, assume that a plane crosses the runway ahead of an aircraft that is in its full power takeoff roll. In order for the aircraft to reach takeoff speed and clear the obstacle, the engines must suddenly operate well above takeoff thrust level. From Figure 1, the *Vehicle Risk Management* block determines the acceleration requirements, which establishes how much thrust is required and for how long. This thrust request and associated acceptable risk are communicated to the *Control Mode Selector and Risk Management* block, which evaluates the request, and selects one of the pre-existing enhanced control strategies (overspeed, in this case) to achieve it. This block also computes information necessary to determine risk, including operating point, defined by fan speed or EPR and ambient conditions, and corresponding steady state values for internal variables that have an impact on part life (speeds, temperatures, and pressures required to produce the desired thrust). The nominal values of these internal variables at the overspeed condition could be looked up, and adjusted up or down based on the estimate of the deterioration level provided by the *Engine Condition Monitoring* block. Now, the pertinent information is sent to the *Engine Life and Operability Risk Assessment* block with the request to analyze the risk of providing the desired level of thrust for the specified time. Since the control mode implementation is specific to the external conditions and the deterioration level of the engine, and the initial risk level depends on the life already consumed, which is provided by the *Engine Condition Monitoring* block, Eq. (6) would be customized and evaluated on a case-by-case basis, using information from the database such as that shown in Figure 4 and Figure 5. For instance, stress, which is a function of rotational speed and distance from the centerline, would be computed for the enhanced control condition and combined with temperature to determine an expected blade life distribution. Many of these distributions would be combined into a single distribution for the blade set, and likewise, the disk life distributions would be combined. This would provide an overall risk for the engine. The computed risk is returned, along with other information such as how long the engine can operate at the stated condition until the acceptable risk level is crossed.

VI. Summary

The paper describes a Risk Assessment Architecture for on-line, real-time analysis of the implementation of an enhanced propulsion control mode in response to an emergency situation. The paper focuses on information flow and the role of the components of the architecture, specifically 1) the database of engine characteristics and properties that are used by the algorithms that compute risk; 2) the algorithms that compute risk, specific to the enhanced control mode to be implemented; and 3) real-time risk information that is a function of the current state of the engine and the specific situation. The information flow was demonstrated through the use of two examples with hypothetical enhanced control modes, one for fast response describing the evaluation process for determining risk of stall, the other for overthrust, demonstrating the calculation of engine life risk. The compelling feature of the architecture is that it computes and returns the risk of using the control mode, independent of the type of control mode. Additionally, because the failure modes are assumed to be independent, their associated risks can be combined if, for instance, there is a desire to implement a fast-responding overthrust control mode. Thus, the Risk Assessment Architecture is generic and control mode independent, only the actual algorithms used and the information they require are control mode specific.

References

[1]National Transportation Safety Board, "Aircraft Accident Report, United Airlines Flight 232, McDonnell Douglas DC-10-10, Sioux Gateway Airport, Sioux City, Iowa, July 19, 1989," PB90-910406, NTSB/AAR-90/06, 1990.

[2]National Transportation Safety Board, "Aircraft Accident Report: Attempted Takeoff From Wrong Runway Comair Flight 5191 Bombardier CL-600-2B19, N431CA Lexington, Kentucky August 27, 2006," NTSB/AAR-07/05, PB2007-910406, 2007.

[3]Guo, T.-H., Litt, J., Merrill, W., and Wood, B., "Fast-Response Engine Research: IRAC Propulsion Task," NASA Aviation Safety Technical Conference, 2008.

[4]Guo, T.-H, and Litt, J. S., "Risk Management for Intelligent Fast Engine Response Control," AIAA-2009-1873, AIAA Infotech@Aerospace Conference, Seattle, WA, April 6-9, 2009.

[5]Federal Aviation Administration FAR Part 33 - Airworthiness Standards: Aircraft Engines, Subpart E--Design and Construction; Turbine Aircraft Engines, Sec. 33-70, Engine life-limited parts.

[6]Federal Aviation Administration FAR Part 33 - Airworthiness Standards: Aircraft Engines, Subpart E--Design and Construction; Turbine Aircraft Engines, Sec. 33-75, Safety analysis.

[7]Federal Aviation Administration FAR Part 33 - Airworthiness Standards: Aircraft Engines, Subpart B--Design and Construction; General, Sec. 33.27, Turbine, compressor, fan, and turbosupercharger rotors.

[8]Federal Aviation Administration FAR Part 33 - Airworthiness Standards: Aircraft Engines, Subpart E--Design and Construction; Turbine Aircraft Engines, Sec. 33.73, Power or thrust response.

[9]Walsh, P. P., and Fletcher, P., *Gas Turbine Performance*, Blackwell Science/ASME, 2004.

[10]Sobey, A. J. and Suggs, A. M., *Control of Aircraft and Missile Powerplants*, John Wiley and Sons, Inc., New York and London, 1963, p. 105.

[11]Zaretsky, E. V., Smith, T., and August, R., "Effect of Design Variables, Temperature Gradients, and Speed on Life and Reliability of a Rotating Disk," NASA TM 88883, March 1987.

[12]Litt, J. S., Frederick, D. K., and Guo, T.-H., "The Case for Intelligent Propulsion Control for Fast Engine Response," AIAA-2009-1876, AIAA Infotech@Aerospace Conference, Seattle, WA, April 6-9, 2009.

[13]Spang, H. A., III, and Brown, H., "Control of Jet Engines," Control Engineering Practice 7, 1999, pp. 1043-1059.

[14]Litt, J. S., and Guo, T.-H., "Fast Thrust Response for Improved Flight/Engine Control under Emergency Conditions," AIAA 2008-6503, AIAA Guidance, Navigation and Control Conference and Exhibit, Honolulu, Hawaii, August 18-21, 2008.

[15]Litt, J. S., "An Optimal Orthogonal Decomposition Method for Kalman Filter-Based Turbofan Engine Thrust Estimation," Journal of Engineering for Gas Turbines and Power, Vol. 130, No. 1, January 2008.

[16]Simon, D. L., and Garg, S., "Optimal Tuner Selection for Kalman Filter-Based Aircraft Engine Performance Estimation," Journal of Engineering for Gas Turbines and Power, Vol. 132, March 2010.

[17]Guo, T.-H., and Litt, J. S., "Resilient Propulsion Control Research for the NASA Integrated Resilient Aircraft Control (IRAC) Project," AIAA-2007-2802, AIAA Infotech@Aerospace, Rohnert Park, CA, May 7-10, 2007.

[18]Bonacuse, P. J., "Retirement for Cause as an Alternate Means of Managing Component Lives," *Research & Technology 1996*, NASA/TM-107350, March 1997.

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-07-2010	Technical Memorandum	

4. TITLE AND SUBTITLE
A Risk Assessment Architecture for Enhanced Engine Operation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Litt, Jonathan, S.; Sharp, Lauren, M.; Guo, Ten-Huei

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
WBS 457280.02.07.03.03.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135-3191

8. PERFORMING ORGANIZATION REPORT NUMBER
E-17402

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITOR'S ACRONYM(S)
NASA

11. SPONSORING/MONITORING REPORT NUMBER
NASA/TM-2010-216776

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category: 07
Available electronically at http://gltrs.grc.nasa.gov
This publication is available from the NASA Center for AeroSpace Information, 443-757-5802

13. SUPPLEMENTARY NOTES

14. ABSTRACT
On very rare occasions, in-flight emergencies have occurred that required the pilot to utilize the aircraft's capabilities to the fullest extent possible, sometimes using actuators in ways for which they were not intended. For instance, when flight control has been lost due to damage to the hydraulic systems, pilots have had to use engine thrust to maneuver the plane to the ground and in for a landing. To assist the pilot in these situations, research is being performed to enhance the engine operation by making it more responsive or able to generate more thrust. Enabled by modification of the propulsion control, enhanced engine operation can increase the probability of a safe landing during an in-flight emergency. However, enhanced engine operation introduces risk as the nominal control limits, such as those on shaft speed, temperature, and acceleration, are exceeded. Therefore, an on-line tool for quantifying this risk must be developed to ensure that the use of an enhanced control mode does not actually increase the overall danger to the aircraft. This paper describes an architecture for the implementation of this tool. It describes the type of data and algorithms required and the information flow, and how the risk based on engine component lifing and operability for enhanced operation is determined.

15. SUBJECT TERMS
Turbofan engine; Control; Actuation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email:help@sti.nasa.gov)
U	U	U	UU	18	19b. TELEPHONE NUMBER *(include area code)* 443-757-5802